

06/15/00
Jc816 U.S. PTO

06-16-00

A

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s): Shawn D. Abbott, Allan D. Anderson, Patrick N. Godding, Maarten G. Punt, and Mehdi Sotoodeh
Docket: 30074.27US11
Title: USB-COMPLIANT PERSONAL KEY USING A SMARTCARD PROCESSOR AND A SMARTCARD READER EMULATOR

CERTIFICATE OF MAILING UNDER 37 CFR 1.10

'Express Mail' mailing label number: EL540750006US

Date of Deposit: June 15, 2000

I hereby certify that this paper or fee is being deposited with the United States Postal Service 'Express Mail Post Office To Addressee' service under 37 CFR 1.10 and is addressed to the Assistant Commissioner for Patents, Washington, D.C. 20231.

By:

Name: Suzie V. McCleave

Jc812 U.S. PTO
09/594456
06/15/00

BOX PATENT APPLICATION
Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

We are transmitting herewith the attached:

- ☒ Transmittal sheet, in duplicate, containing Certificate Of Mailing Under 37 CFR 1.10.
- ☒ Continuation-in-Part Patent Application: Spec. 21 pgs; 19 claims; Abstract 1 pg(s).
The fee has been calculated as shown below in the "Claims as Filed" table.
- ☒ 6 sheets of Drawings
- ☒ An unsigned Combined Declaration and Power of Attorney
- ☒ Our Check No. 3022 in the amount of \$768.00 to cover the Filing Fee
- ☒ Return postcard

CLAIMS AS FILED

Number of Claims Filed	In Excess of:	Number Extra	Rate	Fee
Basic Filing Fee				\$690.00
Total Claims				
19	20	0	x \$18.00 =	\$0.00
Independent Claims				
4	3	1	x \$78.00 =	\$78.00
MULTIPLE DEPENDENT CLAIM FEE				\$0.00
TOTAL FILING FEE				\$768.00

Please charge any additional fees or credit overpayment to Deposit Account No. 50-0494. A duplicate of this sheet is enclosed.

Customer Number 22462.

GATES & COOPER

Howard Hughes Center
6701 Center Drive West, Suite 1050
Los Angeles, CA 90045
(310) 641-8797

By:

Name: Victor G. Cooper

Reg. No.: 39,641

Initials: VGC/sjm

USB-COMPLIANT PERSONAL KEY USING A
SMARTCARD PROCESSOR AND A SMARTCARD READER EMULATOR

CROSS-REFERENCE TO RELATED APPLICATIONS

- 5 This application is a continuation-in-part of U.S. Patent Application No.
09/449,159, filed November 24, 1999, by Shawn D. Abbott, Bahram Afghani, Mehdi
Sotoodeh, Norman L. Denton III, and Calvin W. Long, and entitled "USB-Compliant
Personal Key with Integral Input and Output Devices," which is a continuation-in-part
of U.S. Patent Application No. 09/281,017, filed March 30, 1999 by Shawn D.
10 Abbott, Bahram Afghani, Allan D. Anderson, Patrick N. Godding, Maarten G. Punt,
and Mehdi Sotoodeh, and entitled "USB-Compliant Personal Key," which claims
benefit of U.S. Provisional Patent Application No. 60/116,006, filed January 15, 1999
by Shawn D. Abbott, Barham Afghani, Allan D. Anderson, Patrick N. Godding,
Maarten G. Punt, and Mehdi Sotoodeh, and entitled "USB-Compliant Personal Key,"
15 all of which applications are hereby incorporated by reference herein.

BACKGROUND OF THE INVENTION

1. Field of the Invention

20 The present invention relates to computer peripherals, and in particular to an
inexpensive USB-compliant personal key that is compatible with existing smartcard
processors, drivers, and instruction sets.

2. Description of the Related Art

25 In the last decade, the use of personal computers in both the home and in the
office have become widespread. These computers provide a high level of
functionality to many people at a moderate price, substantially surpassing the
performance of the large mainframe computers of only a few decades ago. The trend
is further evidenced by the increasing popularity of laptop and notebook computers,
which provide high-performance computing power on a mobile basis.

30 The widespread availability of personal computers has had a profound impact
on interpersonal communications as well. Only a decade ago, telephones or fax

machines offered virtually the only media for rapid business communications. Today, a growing number of businesses and individuals communicate via electronic mail (e-mail). Personal computers have also been instrumental in the emergence of the Internet and its growing use as a medium of commerce.

5 While certainly beneficial, the growing use of computers in personal communications, commerce, and business has also given rise to a number of unique challenges. These challenges include the prevention of unauthorized use of software, ensuring the security of e-mail and other electronic communications, as well as Internet commerce.

10 Smartcards represent a longstanding attempt to deal with at least some of the foregoing challenges. Substantial resources have been made in the design and development of smartcards, smartcard readers, and the associated reader/smartcard drivers which allow computer applications to interface with the smartcard to perform security and data storage functions. Even so, smartcards have not enjoyed widespread
15 popularity. Smartcard readers are relatively expensive, and not widely available. Further, the lack of uniform smartcard/smartcard reader physical interface standards have resulted in smartcard/smartcard reader physical interface compatibility problems, many of which remain unresolved.

20 USB-compliant personal keys, such as that which is disclosed in co-pending and commonly assigned U.S. Patent Application Nos. 09/449,159 and 09/281,017, described above, offer the benefit of smartcard functionality in a universally accepted USB form factor. The Universal Serial Bus (USB) is a connectivity standard developed by computer and telecommunication industry members for interfacing computers and peripherals. USB-compliant devices allow the user to install and hot-
25 swap devices without long installation procedures and reboots, and features a 127 device bus capacity, dual-speed data transfer, and can provide limited power to devices attached on the bus. Because the USB connectivity standard is rapidly becoming available on most personal computers, it offers a standard, widely available

physical interface, the unavailability of which has prevented smartcards from achieving widespread acceptance.

While smartcards have not enjoyed widespread popularity in the United States, they are widely accepted in Europe. Hence, many software applications and drivers have been developed for existing smartcard-based devices and their readers. Unfortunately, smartcard interface protocols such as those described in ISO 7816 are incompatible with the USB protocols used in the above-described devices. This incompatibility has led to two unfortunate consequences. First, to comply with USB interface protocol requirements, current USB-compliant personal keys utilize special purpose processors, instead of the low cost, limited capability processors currently available for smartcards. This increases the cost of the USB-compliant personal key, making widespread acceptance more difficult. Also, because each USB-compatible personal key may use a different processor (and different instruction sets), users may require different device drivers for different personal keys. This too represents another barrier to widespread acceptance of the personal key.

From the foregoing, it is apparent that there is a need for a USB-compliant personal key that is usable with legacy personal identification devices, such as processors having smartcard processors and/or those complying with the ISO 7816. There is also a need for a USB-compliant personal key that makes maximum use of existing smartcard protocols, software and devices wherever possible, and which retain at least a limited compatibility with existing devices designed to interface with smartcards. The present invention satisfies that need.

SUMMARY OF THE INVENTION

The present invention satisfies all of these needs with a personal key in a form factor that is compliant with a commonly available I/O interface such as the Universal Serial Bus (USB) and at the same time, usable with existing smartcard software applications. The personal key comprises a USB-compliant interface releaseably coupleable to a host processing device operating under command of an operating

system; a smartcard processor having a smartcard processor-compliant interface for communicating according to a smartcard input and output protocol; and an interface processor, communicatively coupled to the USB-compliant interface and to the smartcard processor-compliant interface, the interface processor implementing a translation module for interpreting USB-compliant messages into smartcard processor-compliant messages and for interpreting smartcard processor-compliant messages into USB-compliant messages.

In one embodiment, the method comprises the steps of accepting a message comprising a smartcard reader command selected from a smartcard reader command set from a host computer operating system in a virtual smartcard reader; packaging the message for transmission via a USB-compliant interface according to a first message transfer protocol; transmitting the packaged message to a personal key communicatively coupled to the USB-compliant interface; receiving the packaged message in the personal key; unpackaging the message in the personal key to recover the smartcard reader command; translating the smartcard reader command into a smartcard command within the personal key; and providing the smartcard command to the smartcard processor.

The present invention is well suited for controlling access to network services, or anywhere a password, cookie, digital certificate, or smartcard might otherwise be used, including:

- Remote access servers, including Internet protocol security (IPSec), point to point tunneling protocol (PPTP), password authentication protocol (PAP), challenge handshake authentication protocol (CHAP), remote access dial-in user service (RADIUS), terminal access controller access control system (TACACS);
- Providing Extranet and subscription-based web access control, including hypertext transport protocol (HTTP), secure sockets layer (SSL);
- Supporting secure online banking, benefits administration, account management;

- Supporting secure workflow and supply chain integration (form signing);
- Preventing laptop computer theft (requiring personal key for laptop operation);
- Workstation logon authorization;
- 5 • Preventing the modification or copying of software;
- Encrypting files;
- Supporting secure e-mail, for example, with secure multipurpose Internet mail extensions (S/MIME), and open pretty good privacy (OpenPGP);
- Administering network equipment administration; and
- 10 • Electronic wallets, with, for example, secure electronic transaction (SET, MilliCent, eWallet)

BRIEF DESCRIPTION OF THE DRAWINGS

Referring now to the drawings in which like reference numbers represent
15 corresponding parts throughout:

FIG. 1 is a diagram showing an exemplary hardware environment for practicing the present invention;

FIG. 2 is a block diagram of a personal key communicatively coupled to a host computer;

20 FIG. 3 is a block diagram of a personal key with a smartcard processor communicatively coupled to a host computer; and

FIGs. 4A-4D are flow charts presenting exemplary method steps that can be used to practice the present invention.

25 DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

In the following description, reference is made to the accompanying drawings which form a part hereof, and which is shown, by way of illustration, several embodiments of the present invention. It is understood that other embodiments may

be utilized and structural changes may be made without departing from the scope of the present invention.

FIG. 1 illustrates an exemplary computer system 100 that could be used to implement the present invention. The host computer 102 comprises a processor 104 and a memory, such as random access memory (RAM) 106. The host computer 102 is operatively coupled to a display 122, which presents images such as windows to the user on a graphical user interface 118B. The host computer 102 may be coupled to other devices, such as a keyboard 114, a mouse device 116, a printer 128, etc. Of course, those skilled in the art will recognize that any combination of the above components, or any number of different components, peripherals, and other devices, may be used with the host computer 102.

Generally, the host computer 102 operates under control of an operating system 108 stored in the memory 106, and interfaces with the user to accept inputs and commands and to present results through a graphical user interface (GUI) module 118A. Although the GUI module 118A is depicted as a separate module, the instructions performing the GUI functions can be resident or distributed in the operating system 108, the computer program 110, or implemented with special purpose memory and processors. The host computer 102 also implements a compiler 112 which allows an application program 110 written in a programming language such as COBOL, C++, FORTRAN, or other language to be translated into processor 104 readable code. After completion, the application 110 accesses and manipulates data stored in the memory 106 of the host computer 102 using the relationships and logic that are generated using the compiler 112. The host computer 102 also comprises an input/output (I/O) port for a personal token 200 (hereinafter alternatively referred to also as a personal key 200). In one embodiment, the I/O port is a USB-compliant interface comprising a host computer USB-compliant interface 130A and a personal token USB-compliant interface 130B (hereinafter referred to collectively as the USB-compliant interface 130).

005944E-061500
005790-934550

In one embodiment, instructions implementing the operating system 108, the computer program 110, and the compiler 112 are tangibly embodied in a computer-readable medium, e.g., data storage device 120, which could include one or more fixed or removable data storage devices, such as a zip drive, floppy disc drive 124,
5 hard drive, CD-ROM drive, tape drive, etc. Further, the operating system 108 and the computer program 110 are comprised of instructions which, when read and executed by the computer 102, causes the computer 102 to perform the steps necessary to implement and/or use the present invention. Computer program 110 and/or operating instructions may also be tangibly embodied in memory 106 and/or data
10 communications devices, thereby making a computer program product or article of manufacture according to the invention. As such, the terms "article of manufacture" and "computer program product" as used herein are intended to encompass a computer program accessible from any computer readable device or media.

The host computer 102 may be communicatively coupled to a remote
15 computer or server 134 via communication medium 132 such as a dial-up network, a wide area network (WAN), local area network (LAN), virtual private network (VPN) or the Internet. Program instructions for computer operation, including additional or alternative application programs can be loaded from the remote computer/server 134. In one embodiment, the computer 102 implements an Internet browser, allowing the
20 user to access the world wide web (WWW) and other internet resources.

Those skilled in the art will recognize that many modifications may be made to this configuration without departing from the scope of the present invention. For example, those skilled in the art will recognize that any combination of the above components, or any number of different components, peripherals, and other devices,
25 may be used with the present invention.

FIG. 2 is a block diagram illustrating the components of one embodiment of a personal key 200. The personal key 200 communicates with and obtains power from the host computer 102 through a USB-compliant communication path in the USB-compliant interface 130 which includes the input/output port 130A of the host

computer 102 and a matching input/output (I/O) port 130B on the personal key 200. The processor 212 is communicatively coupled to a memory 214, which stores data and instructions to implement the above-described features of the invention. In one embodiment, the memory 214 is a non-volatile random-access memory that can retain
5 factory-supplied data as well as customer-supplied application related data. The processor 212 may also include some internal memory for performing some of these functions.

The processor 212 is optionally communicatively coupled to an input device 218 via an input device communication path 224 and to an output device 222 via an
10 output device communication path 224, both of which are distinct from the USB-compliant interface 130. These separate communication paths 220 and 224 allow the user to view information about processor 212 operations and provide input related to processor 212 operations without allowing a process or other entity with visibility to the USB-compliant interface 130 to eavesdrop or intercede. This permits secure
15 communications between the key processor 212 and the user. In one embodiment of the invention set forth more fully below, the user communicates directly with the processor 212 by physical manipulation of mechanical switches or devices actuatable from the external side of the key (for example, by pressure-sensitive devices such as buttons and mechanical switches). In another embodiment of the invention set forth
20 more fully below, the input device includes a wheel with tactile detents indicating the selection of characters.

The input device and output devices 218, 222 may cooperatively interact with one another to enhance the functionality of the personal key 200. For example, the output device 222 may provide information prompting the user to enter information
25 into the input device 218. For example, the output device 222 may comprise a visual display such as an alphanumeric LED or LCD display (which can display Arabic numbers and or letters) and/or an aural device. The user may be prompted to enter information by a beeping of the aural device, by a flashing pattern of the LED, or by both. The output device 222 may also optionally be used to confirm entry of

information by the input device 218. For example, an aural output device may beep when the user enters information into the input device 218 or when the user input is invalid. The input device 218 may take one of many forms, including different combinations of input devices.

5 Although the input device communication path 220 and the output device communication path 224 are illustrated in FIG. 2 as separate paths, the present invention can be implemented by combining the paths 220 and 224 while still retaining a communication path distinct from the USB-compliant interface 130. For example, the input device 218 and output device 222 may be packaged in a single
10 device and communications with the processor 212 multiplexed over a single communication path.

FIG. 3 is a block diagram of the personal key 300 and host computer 102 as applied to the present invention. Unlike the personal key 200 illustrated in FIG. 2, the personal key 300 illustrated in FIG. 3 comprises a smartcard processor 320. The
15 smartcard processor 320 is a processor which complies with well-known smartcard I/O protocols and smartcard command sets and functions, such as those described by the International Standards Organization (ISO) standard 7816 Part III (defining electronic properties and transmission characteristics), which is hereby incorporated by reference herein.

20 Physically, the smartcard compliant I/O interface 324 includes a serial I/O line, a reset (RST) line, a clock (CLK) line, a programming voltage (VPP), a power supply voltage (VCC) and a ground. This I/O interface 324 is further described in the publication "Introduction to Smartcards" by Dr. David B. Everett, which was published in 1999 by the Smart Card News Ltd., and is incorporated by reference
25 herein.

As was the case with the personal key 200 and host computer 102 illustrated in FIG. 1, the present invention allows the use of a personal key 300 communicating with the host computer 102 via a USB-compliant interface 130. However, the substitution of the smartcard processor 320 for the ordinary processor 212 depicted in

FIG. 2 has several advantages. First, smartcard processors 320 are relatively inexpensive and readily available. Second, a large number of application programs 110 have been developed for the use of smartcards, including the personal computer/smartcard (PC/SC) interface developed by the MICROSOFT

5 CORPORATION. By providing a smartcard processor (which complies with the smartcard I/O protocols and supports smartcard command sets), this software can be used with a personal key 300 in a USB-compliant form factor.

The use of the smartcard processor 320 in the personal key 300 is enabled by use of an interface processor 314 communicatively coupled to the smartcard processor 10 320 via a smartcard-compatible (S/C 7816) interface 324. The interface processor 314 comprises a smartcard reader emulator module (SREM) 316 and a translation module 318. The SREM 316 implements functions that emulate those of a smartcard reader, thus projecting the image of a smartcard reader to the smartcard processor 320. The SREM 316 provides all instructions and commands to the smartcard 15 processor 320 and receives messages and responses from the smartcard processor 320 according to the S/C protocol.

The host computer 102 comprises a virtual smartcard reader module (VSRM) 302. The VSRM comprises a communication module 312, an answer-to-reset module 308, and a smartcard insertion/removal reporting module 306. The communication 20 module 312 packages messages intended for the personal key 300 for transmission via the USB-compliant interface. In one embodiment, messages and commands that are sent to the personal key 300 packaged as:

USB command = USB header + USB cdata (wherein USB cdata is the smartcard 25 compliant command)

and messages and responses from the personal key 300 are packaged as:

USB response = USB header + USB rdata (wherein USB rdata is the smartcard compliant response)

These packaged messages are unpacked by the translation module 318 in the personal key 300. Similarly, messages transmitted by the smartcard processor 320 to the host computer 102 are packaged by the translation module 318 and unpacked by the communication module 312 before being provided to the operating system 108, the application program interface 260, and the application 110 using the personal key 300 to perform operations.

Just as the SREM 316 emulates the presence of a smartcard reader for the smartcard processor 320, the VSRM 302 emulates the presence of a smartcard reader to the OS 108 in the host computer 102. These functions are accomplished in the bootup module 311, the insert/remove module 306, the answer-to-reset module 308, and the PTS module 310.

As a part of a normal bootup sequence, the host computer's 102 operating system performs a startup sequence to determine which hardware elements are available for use. In prior art smartcard systems, the smartcard reader remains coupled to the host computer 102, whether a smartcard is inserted into the reader or not. Hence, the smartcard reader can respond to startup sequence queries, and the smartcard reader is recognized by the operating system 108 for further operations. However, in the present invention, there is no smartcard reader to answer to the bootup query, and the operating system would ordinarily be unable to operate with a smartcard thereafter. To solve this problem, the present invention comprises a bootup module 311, which responds to messages from the operating system 108 in the same way as a smartcard reader would if it were coupled to the host computer 102.

Similarly, the insert/remove module 306 provides an indication to the operating system 108 that the personal key 300 has been inserted or removed from the USB-compliant interface 130. This is accomplished by querying the host computer USB-compliant interface port 130A.

When a software application calls 110, via API 260 and the operating system 108 invokes a command that calls for a smartcard related function, the smartcard reader passes a reset command to the smartcard. The smartcard returns an answer-to-reset message which indicates, among other things, the protocol and I/O interface
5 supported by the attached smartcard.

The reset signal is used to start up the program contained in a memory 322 communicatively coupled to or resident within the smartcard processor 320. The ISO standard defines three reset modes, internal reset, active low reset, and synchronous high active reset. Most smartcard processors 320 operate using the active low reset
10 mode. In this mode, the smartcard processor 320 transfers control to the entry address for the program when the reset signal returns to the high voltage level. The synchronous mode of operation is more commonly met with smartcards used for telephonic applications.

The sequence of operations for activating the smartcard processor 320 is
15 defined in order to minimize the possibility of damaging the smartcard processor 320. Of particular importance is avoiding corruption of the non-volatile memory 322 of the smartcard. Most smartcard processors 320 operate using an active low reset mode in which the smartcard processor 320 transfers control to the entry address for the program when the reset signal returns to the high voltage level. The sequence
20 performed by the smartcard processor includes the steps of setting the RST line low, applying VCC to the proper supply voltage, setting the I/O in the receive mode, setting VPP in the idle mode, applying the clock, and taking the RST line high (active low reset).

In prior art smartcard systems, after the reset signal is applied by the smartcard
25 reader, the smartcard processor 320 responds with an answer-to-reset message. For the active low reset mode, the smartcard processor 320 should respond between 400 and 40,000 clock cycles after the rising edge of the reset signal. The answer-to-reset signal is at most 33 characters, and includes 5 fields including an initial character (TS), a format character (TO), interface characters (TAi, TBi, TCi, and TDi),

historical characters (T1, T2, ... , TK), and a check character (TCK). Among other things, the answer-to-reset signal provides an indication of the smartcard protocol(s) which are supported smartcard processor. Typical smartcard protocols include the T=0 protocol (asynchronous half duplex byte transmission) and T=1 (asynchronous
5 half duplex block transmission).

In the embodiment of the present invention shown in FIG. 3, the reset signal is provided by the VSRM 302, packaged by the communication module 312, and sent via the USB-compliant interface 130B to the personal key 300. The message is unwrapped by the translation module 318. Then, the smartcard reader emulation
10 module activates the RST signal path in the smartcard interface 324, thus providing the RST command to the smartcard processor 320. The smartcard processor 320 responds with an answer-to-reset message, sends the message via the serial I/O line of the smartcard interface 324 to the interface processor 314. The message is then packaged by the translation module 318 and transmitted to the host computer 102 via
15 the USB-compliant interface 326. The message is then unpackaged by the communication module 312 and provided to the operating system 108 and ultimately, the application 110 that requested the use of the smartcard.

In another embodiment of the present invention, the personal key 300 does not comprise a smartcard processor 320, but rather a special purpose processor which
20 does not respond to messages and commands in the smartcard I/O protocol (such as that which is illustrated in FIG. 1). The present invention can still be used with existing smartcard applications 110, however, because the VSRM 302 and the interface processor 314 can be used to simulate the presence of a smartcard processor 320. When the smartcard software application 110 desires use of the personal key
25 300, the VSRM accepts the reset command from the PC/SC modules in the operating system 108, translates the reset message into a functionally equivalent message for the special purpose processor in the personal key 300, and transmits the message to the personal key 300. After the personal key 300 is activated, it sends a message indicating as such to the host computer 102. The VSRM 302, and translates this

message to a response that is compatible with the smartcard application 110, namely, an ATR message. Alternatively, the smartcard command to special purpose processor command translation can occur in the emulation processor 314 in the personal key 300.

5 Returning to the embodiment disclosed in FIG. 3, after the smartcard processor has issued the ATR message, a protocol type selection (PTS) message may be sent to the smartcard processor 320. The PTS message from the OS 108 is received by the PTS module 310 in the VSRM 302, packaged for transmission via the USB-compliant interface 130 to the personal key 300, where it is unpackaged and
10 provided to the smartcard processor 320. The smartcard provides a response consistent with the ISO standards to the emulation module 316. The response is packaged, and transmitted over the USB-compliant interface 130 to the host computer 102, where it is unpackaged by the communication module 312 and provided to the operating system.

15 FIGs. 4A-4D are flow charts presenting exemplary method steps used to practice one embodiment of the present invention. When the host computer 102 is booted up, the virtual smartcard reader 302 accepts 402 a bootup query from the host computer's operating system 108. Although a smartcard reader is not communicatively coupled to the host computer 130 the virtual smartcard reader 302
20 emulates the existence of a smartcard reader and provides an indication that a smartcard reader is available to the OS 108. Consequently, when the bootup procedures are completed, a smartcard reader will be registered as an available device to smartcard applications 110.

25 When the host computer is booted up, a personal key 300 may or may not be communicatively coupled to the USB-compliant interface 130. When a personal key 300 is not attached, the VSRM 302 provides 404 the same indication to the operating system 108 as would be supplied by a smartcard reader without an inserted smartcard. This is accomplished by receiving 406 an indication that the personal key has been communicatively coupled to the USB-compliant interface, and providing an

indication to the host computer operating system. Since the VSRM is emulating the functions of a smartcard, the indication is provided 408 to the host computer operating system (or equivalently, the personal computer/smartcard (PC/SC) interface modules therein) is that of an insert event.

5 If desired and the smartcard processor 320 supports multiple protocols, a protocol type selection (PTS) command may be issued by the operating system 108. The VSRM 302 receives 410 the PTS command, packages the command for transmission to the personal key 300 via the USB-compliant interface 130. The wrapped PTS command is then transmitted over the USB-compliant interface 130 and
10 received by the personal key 300. The PTS command is unwrapped by the translate module 318 in the interface processor 314 and provided to the smartcard processor 320 via the smartcard-compliant interface 324. The smartcard processor computes the appropriate response, sends the response to the interface processor 314, where the response is packaged by the translate module 318 for transmission to the host
15 computer 102 via the USB-compliant interface 130. The communication module 312 unpackages the response, and the PTS module 310 formats the response, if necessary, to be consistent with a PTS response received from a smartcard reader. The formatted response is then provided 412 to the OS 108.

FIG. 4B is a flow chart describing exemplary method steps used to provide
20 commands and/or data from the OS 108 to the smartcard processor 320 and from the smartcard processor 320 to the OS 108. A message, which may comprise a smartcard reader command belonging to a smartcard reader command set is accepted 414 from a host computer operating system 108 in the virtual smartcard reader module (VSRM) 302. The message is packaged 416 for transmission via the USB-compliant interface
25 130 according to a first message transfer protocol.

The packaged message is then transmitted 418 to the communicatively coupled personal key 300 via the USB-compliant interface 130. The packaged message is received 420 and unpackaged 422 in the personal key 300. If the smartcard reader command requires additional processing before being forwarded to

the smartcard processor 320, the smartcard reader command is translated 424 into a smartcard command within the personal key 300 before being provided 426 to the smartcard processor 320.

5 The smartcard processor 320 then performs the indicated operation, and a response is accepted 428 from the smartcard processor 320. If the smartcard response requires further processing by a smartcard reader, the smartcard response is translated 430 into a smartcard reader response. The smartcard reader response is then packaged 432 and transmitted 434 to the host computer 102 via the USB-compliant interface 130. The host computer 102 receives 436 and unpackages 438 the message and
10 provides 440 the response to the smartcard software application 110 that issued the command.

Next, when the personal key 300 is removed, the VSRM 302 reports 444 an indication to the OS 108 that the “virtual smartcard” (the personal key 300) has been removed. The provided indication is the same as that which would be provided by a
15 smartcard reader when a smartcard is removed. The indication can be obtained, for example by receiving 442 an indication from a USB driver or other device indicating the removal of a USB device.

Tables I and II provide a summary of the communication protocol for an OS 108 command from the host computer 102 to the smartcard processor 320 in the
20 personal key (Table I), and for a smartcard processor 320 response to the operating system 108.

Step	Description
1	Smartcard reader command issued from OS 108 is passed to VSRM 302
2	VSRM 302 adds a USB header, and creates a USB command
3	VSRM's 302 communication module 312 sends the USB command to the personal key 300
4	The translation module 318 strips off the USB header and recovers the smartcard command
5	The smartcard command is sent to the smartcard processor 320
6	The smartcard processor 320 executes the function requested by the smartcard command

Table I

Step	Description
1	Smartcard processor 320 generates a smartcard response
2	The smartcard response is sent from the smartcard processor 320 to the translation module 318
3	The translation module 318 adds a USB header to create a USB response
4	The USB response is transmitted to the VSRM 302
5	The communication module 312 strips off the USB header and recovers the smartcard response
6	The smartcard response is transmitted to the OS 108

Table II

Tables III and IV provide a summary of the communication protocol for a request from an application program 110 to the smartcard processor 320 and for a request from an application program 110 to the smartcard processor 320.

Step	Description
1	Smartcard processor 320 command from the application program 110 is sent to the OS 108 via an API 260
2	The smartcard processor 320 command is sent from the OS 108 to the VSRM 302
3	The VSRM 302 adds a USB header to the smartcard processor 320 command to create a USB-compatible command
4	The VSRM's comm module 312 sends the USB-compliant command to the personal key 300
5	Translation module 318 strips off the USB header and recovers the smartcard processor command
6	The smartcard processor command is transmitted to the smartcard processor 320
7	The smartcard processor 320 performs the function indicated by the smartcard processor command

Table III

Step	Description
1	The smartcard processor 320 generates a response to the smartcard processor command
2	The response is provided to the translation module 318
3	The translation module adds a USB header to create a USB-compatible smartcard processor response
4	The USB-compatible smartcard processor response is sent to the VSRM 302
5	The communication module 312 strips off the USB header to recover the smartcard processor response
6	The smartcard processor response is provided to the application 110 via the OS 108 and the API 260

Table IV

5

Conclusion

This concludes the description of the preferred embodiments of the present invention. In summary, the present invention describes a personal key comprising a USB-compliant interface releaseably coupleable to a host processing device operating under command of an operating system; a smartcard processor having a smartcard processor-compliant interface for communicating according to a smartcard input and output protocol; and an interface processor, communicatively coupled to the USB-compliant interface and to the smartcard processor-compliant interface, the interface processor implementing a translation module for interpreting USB-compliant

10

messages into smartcard processor-compliant messages and for interpreting smartcard processor-compliant messages into USB-compliant messages. In another embodiment, the invention is described by a method comprising the steps of accepting a message comprising a smartcard reader command selected from a smartcard reader command set from a host computer operating system in a virtual smartcard reader; packaging the message for transmission via a USB-compliant interface according to a first message transfer protocol; transmitting the packaged message to a personal key communicatively coupled to the USB-compliant interface; receiving the packaged message in the personal key; unpackaging the message in the personal key to recover the smartcard reader command; translating the smartcard reader command into a smartcard command within the personal key; and providing the smartcard command to the smartcard processor.

The foregoing description of the preferred embodiment of the invention has been presented for the purposes of illustration and description. It is not intended to be exhaustive or to limit the invention to the precise form disclosed. Many modifications and variations are possible in light of the above teaching. It is intended that the scope of the invention be limited not by this detailed description, but rather by the claims appended hereto. The above specification, examples and data provide a complete description of the manufacture and use of the composition of the invention. Since many embodiments of the invention can be made without departing from the spirit and scope of the invention, the invention resides in the claims hereinafter appended.

WHAT IS CLAIMED IS:

1. A compact personal token, comprising:
 - a USB-compliant interface releaseably coupleable to a host processing device operating under command of an operating system;
 - 5 a smartcard processor having a smartcard processor-compliant interface for communicating according to a smartcard input and output protocol;
 - an interface processor, communicatively coupled to the USB-compliant interface and to smartcard processor-compliant interface the interface processor implementing a translation module for interpreting USB-compliant messages into smartcard processor-compliant messages and for interpreting smartcard processor-compliant messages into USB-compliant messages.
- 10 2. The apparatus of claim 1, wherein the interface processor emulates a smartcard reader to the smartcard processor.
- 15 3. The apparatus of claim 1, wherein:
 - the host processing device comprises a virtual smartcard reader in communication with the operating system, the virtual smartcard reader for emulating a smartcard reader communicatively coupled to the host processing device and
 - 20 including a communication module for packaging messages for transmission to the personal token via the USB compliant interface according to a first protocol and for unpackaging messages received from the personal token via the USB-compliant interface according to the first protocol; and
 - the interface processor translation module unpackages messages from the host
 - 25 processing device according to the first protocol and packages messages destined for the host processing device according to the first protocol.

4. The apparatus of claim 3, wherein the virtual smartcard reader further comprises a bootup module for responding to an operating system bootup procedure with an indication that a smartcard reader is communicatively coupled to the host processor.

5

5. The apparatus of claim 3, wherein the virtual smartcard reader further comprises an answer-to-reset (ATR) module for providing an ATR message to the operating system in response to a reset message.

10

6. The apparatus of claim 3, wherein the virtual smartcard reader further comprises a reporting module for receiving and reporting the insertion of the personal token in a USB-compliant port communicatively coupled to the host processor and the removal of the personal token as a removal of a smartcard from a smartcard reader.

15

7. The apparatus of claim 3, wherein the virtual smartcard reader further comprises a protocol selection module for receiving a protocol type selection (PTS) command from the operating system and providing a PTS response message to the operating system.

20

8. A host processing device, comprising:

a processor;

a memory, communicatively coupled to the processor, the memory storing processor operation commands implementing an operating system; and

25

a virtual smartcard reader module stored in the memory and in communication with the operating system, for emulating at least one smartcard reader to the operating system.

9. The apparatus of claim 8, wherein the virtual smartcard reader module comprises a communication module for packaging messages for transmission to a personal token communicatively coupled to the host processor via a USB-compliant interface and for unpacking messages received from the personal token.

5

10. The apparatus of claim 8, wherein the virtual smartcard reader comprises a bootup module for responding to an operating system bootup procedure with an indication that a smartcard reader is communicatively coupled to the host processor.

10

11. The apparatus of claim 8, further comprising an answer-to-reset (ATR) module providing an ATR message to the operating system in response to a reset message.

15

12. The apparatus of claim 8, wherein the virtual smartcard reader further comprises a reporting module for receiving and reporting the insertion of a personal token in a USB compliant port communicatively coupled to the host processor and the removal of the personal token as a removal of a smartcard from a smartcard reader.

20

13. The apparatus of claim 8, wherein the virtual smartcard reader further comprises a protocol selection module for receiving a protocol type selection (PTS) command from the operating system and providing a PTS response message to the operating system.

14. A method of communicating with a smartcard processor in a personal key communicatively coupled to a host computer via a USB-compliant interface, comprising the steps of:

5 accepting a message comprising a smartcard reader command selected from a smartcard reader command set from a host computer operating system in a virtual smartcard reader;

packaging the message for transmission via a USB-compliant interface according to a first message transfer protocol;

10 transmitting the packaged message to a personal key communicatively coupled to the USB-compliant interface;

receiving the packaged message in the personal key;

unpackaging the message in the personal key to recover the smartcard reader command;

15 translating the smartcard reader command into a smartcard command within the personal key; and

providing the smartcard command to the smartcard processor.

15. The method of claim 14, further comprising the steps of:

accepting a smartcard response from the smartcard processor;

20 translating the smartcard response into a smartcard reader response;

packaging the smartcard reader response for transmission to the host processor via the USB-compliant interface;

transmitting the packaged message from the personal key to the host processor;

25 receiving the packaged message in the host computer;

unpackaging the smartcard reader response; and

providing the smartcard reader response to the host processor operating system.

16. The method of claim 14, further comprising the steps of:
accepting a startup query from the host computer operating system in the
virtual smartcard reader; and
providing an indication that a smartcard reader is communicatively coupled to
5 the host computer to the host computer operating system.

17. The method of claim 16, further comprising the steps of:
receiving an indication that the personal key has been communicatively
coupled to the USB-compliant interface;
10 reporting the indication that the personal key is communicatively coupled to
the USB-compliant interface to the host processor operating system as the insertion of
a smartcard;
receiving an indication that the personal key has been communicatively
decoupled from the USB-compliant interface; and
15 reporting the indication that the personal key has been communicatively
decoupled from the USB-compliant interface to the host processor operating system
as the removal of the smartcard.

18. The method of claim 14, further comprising the steps of:
20 receiving a protocol type selection (PTS) command from the host computer
operating system; and
providing a PTS response message to the operating system.

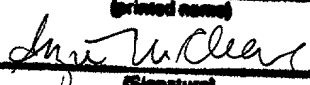
005790" 9544560

- 5

ABSTRACT OF THE DISCLOSURE

A compact, self-contained, personal key is disclosed. The personal key comprises a USB-compliant interface releaseably coupleable to a host processing device operating under command of an operating system; a smartcard processor
5 having a smartcard processor-compliant interface for communicating according to a smartcard input and output protocol; and an interface processor, communicatively coupled to the USB-compliant interface and to the smartcard processor-compliant interface, the interface processor implementing a translation module for interpreting USB-compliant messages into smartcard processor-compliant messages and for
10 interpreting smartcard processor-compliant messages into USB-compliant messages.

005790" 954456 061500

"Express Mail" mailing label number EL54075000645
Date of Deposit JUNE 15, 2000
I hereby certify that this paper or fee is being deposited with the United States Postal Service "Express Post Office to Addressee" service under 37 CFR 1.10 on the date indicated above and is addressed to:
Assistant Commissioner for Patents, Washington, D.C. 20231.
• SUZIE MC CLEAVE
(printed name)

(Signature)

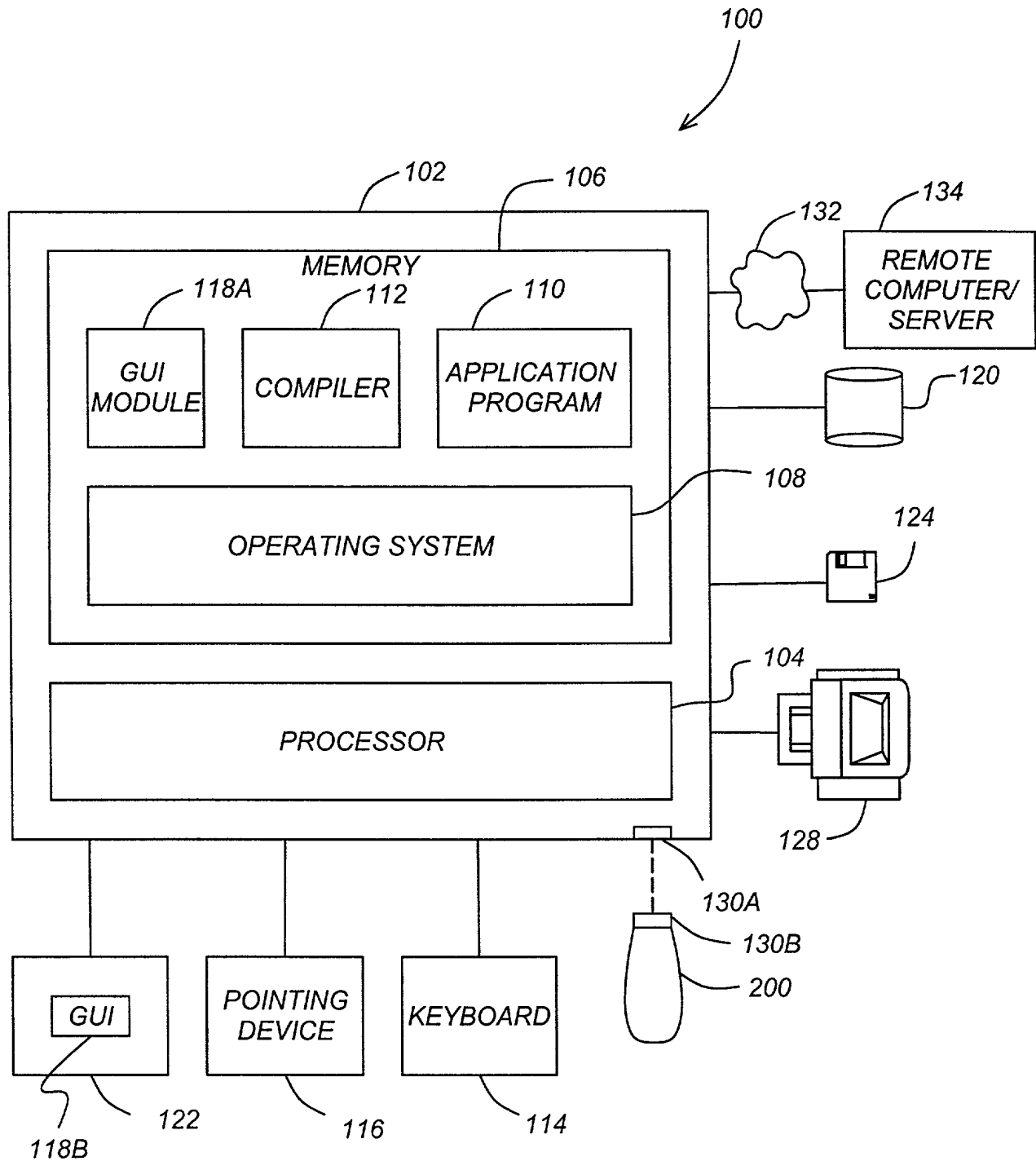


FIG. 1

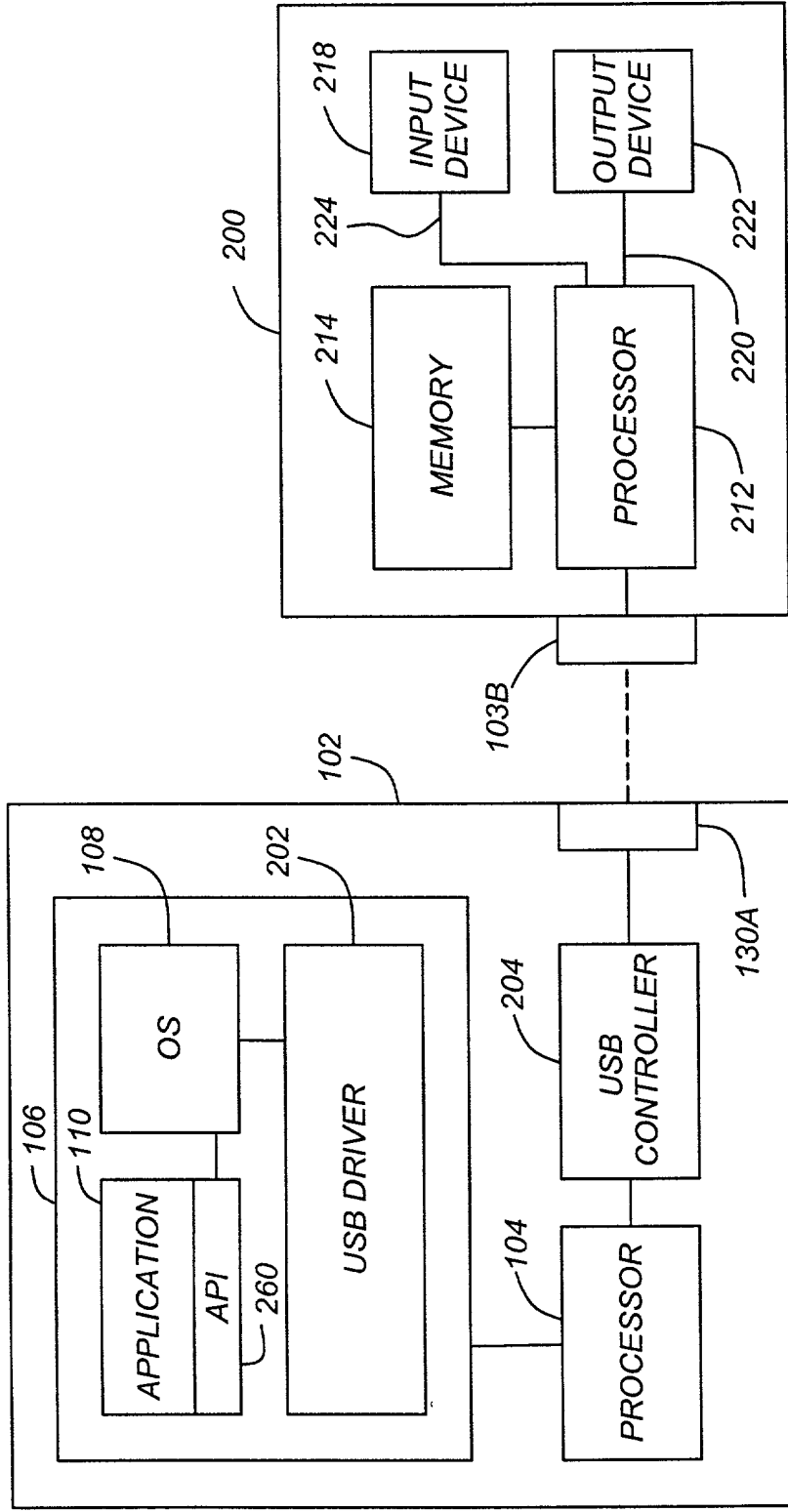
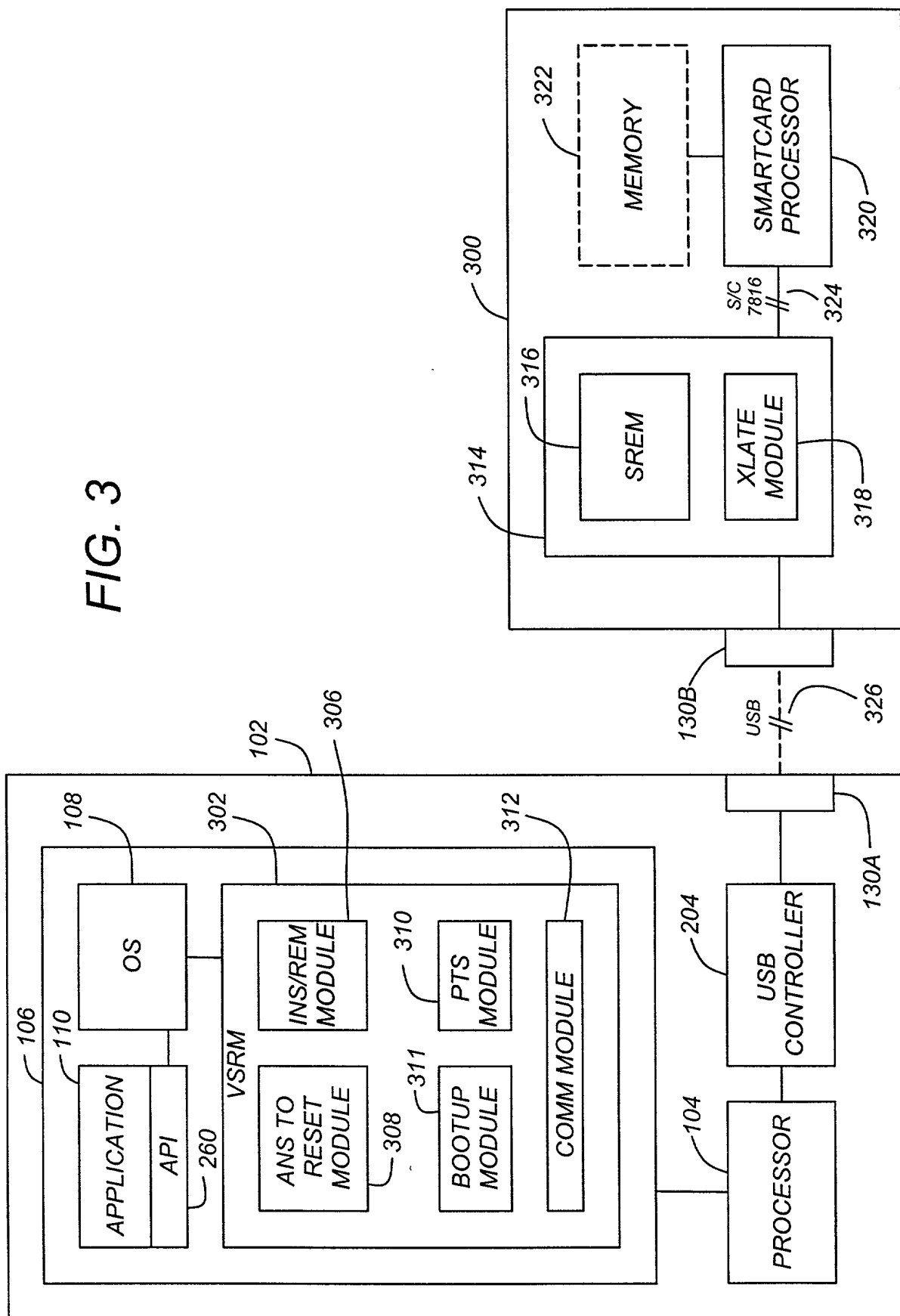


FIG. 2

FIG. 3



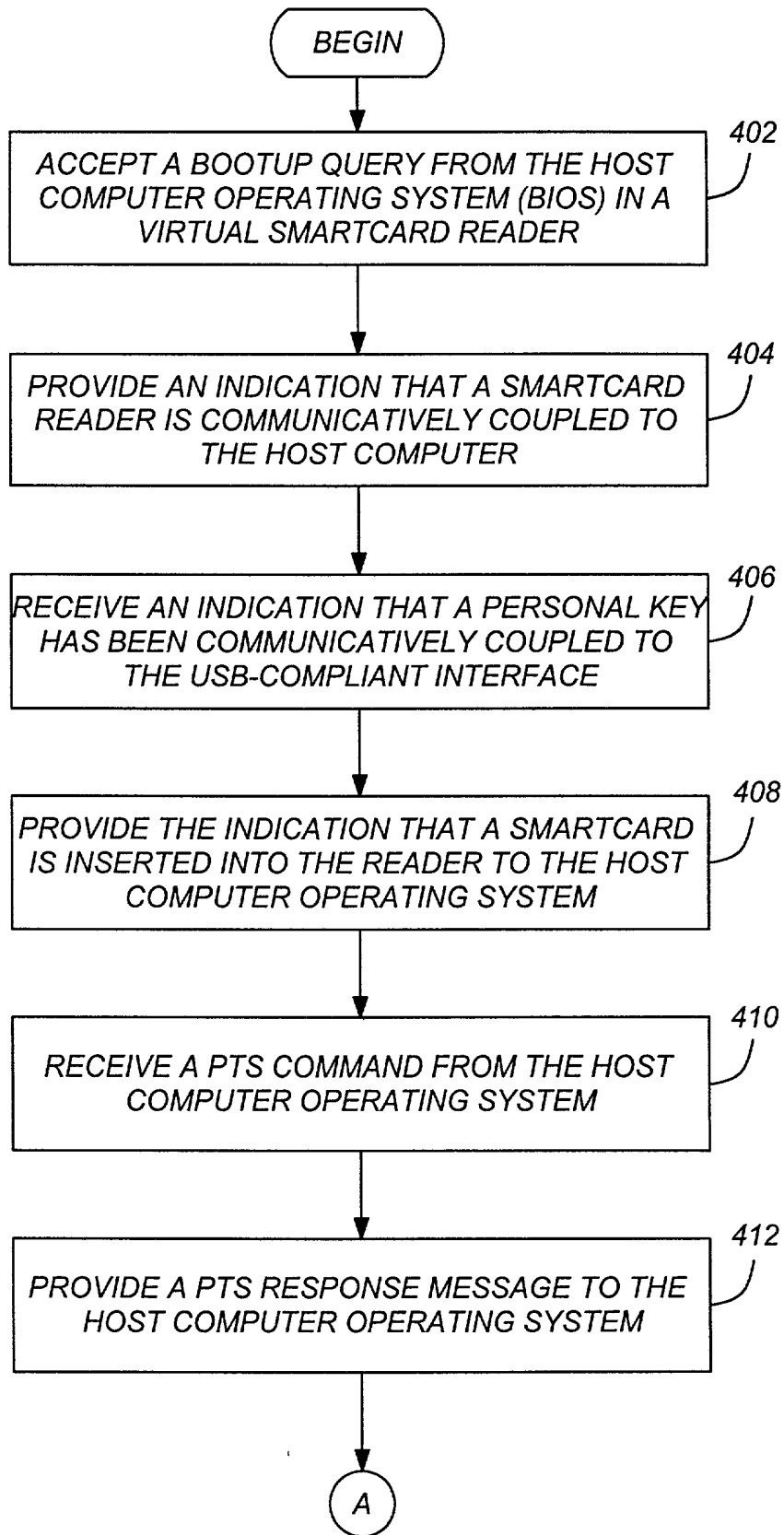
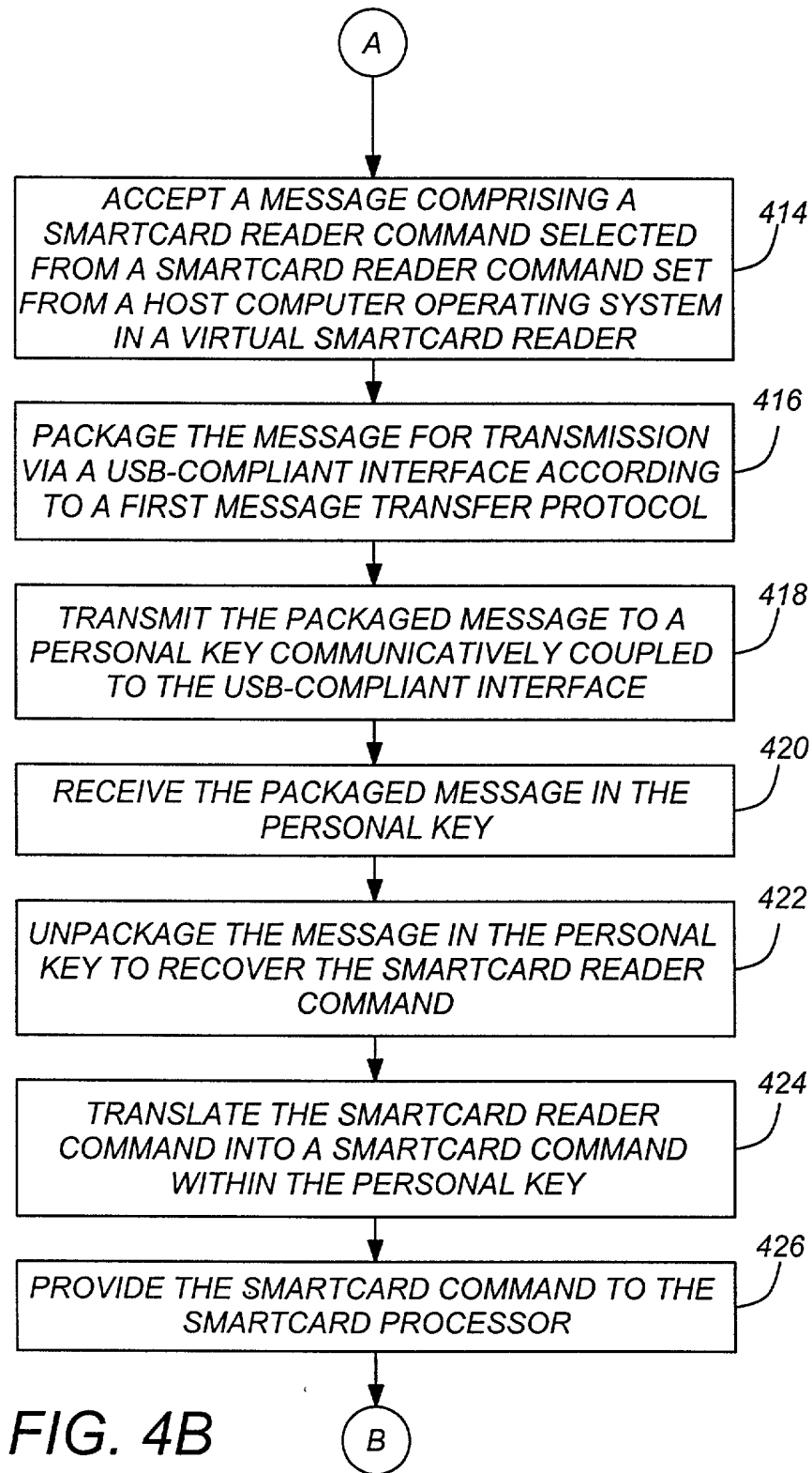


FIG. 4A



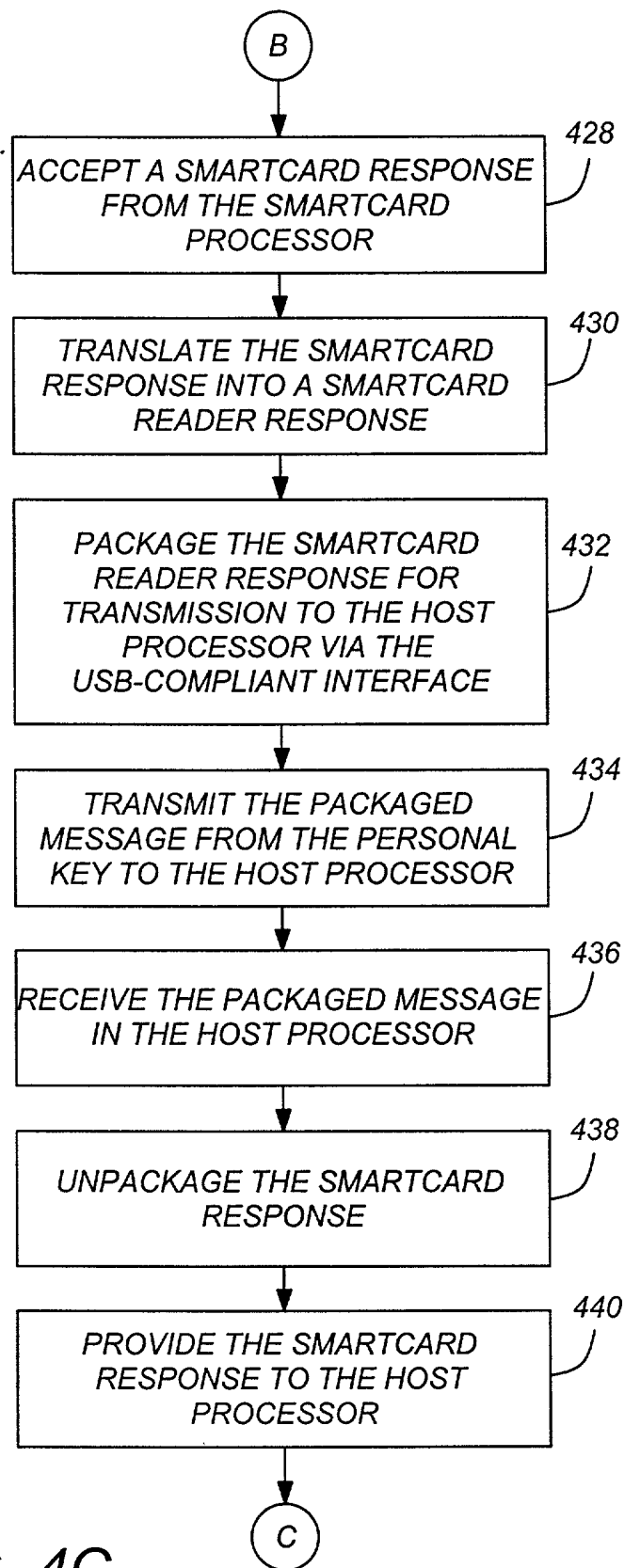


FIG. 4C

GATES & COOPER

United States Patent Application

COMBINED DECLARATION AND POWER OF ATTORNEY

As a below named inventor I hereby declare that: my residence, post office address and citizenship are as stated below next to my name; that

I verily believe I am the original, first and sole inventor (if only one name is listed below) or a joint inventor (if plural inventors are named below) of the subject matter which is claimed and for which a patent is sought on the invention entitled:

USB-COMPLIANT PERSONAL KEY USING A SMARTCARD PROCESSOR AND A SMARTCARD
READER EMULATOR

The specification of which:

a. ☒ is attached hereto.

b. ☐ was filed on _____ as United States Application Number or PCT International Application Number _____ and was amended on _____ (if applicable), which I have reviewed and for which I solicit a United States patent.

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to the patentability of this application in accordance with Title 37, Code of Federal Regulations, § 1.56 (attached hereto).

I hereby claim foreign priority benefits under Title 35, United States Code, § 119(a)-(d) or 365(b) of any foreign application(s) for patent or inventor's certificate or 365(a) of any PCT international application which designated at least one country other than the United States of America, listed below and have also identified below any foreign application for patent or inventor's certificate or any PCT application having a filing date before that of the application on the basis of which priority is claimed:

a. ☒ no such applications have been filed.

b. ☐ such applications have been filed as follows:

FOREIGN APPLICATION(S), IF ANY, CLAIMING PRIORITY UNDER 35 USC § 119			
COUNTRY	APPLICATION NUMBER	DATE OF FILING (day, month, year)	DATE OF ISSUE (day, month, year)
OTHER FOREIGN APPLICATION(S), IF ANY, FILED BEFORE THE PRIORITY APPLICATION(S)			
COUNTRY	APPLICATION NUMBER	DATE OF FILING (day, month, year)	DATE OF ISSUE (day, month, year)

I hereby claim the benefit under Title 35, United States Code, § 120 of any United States application(s), or 365(c) of any PCT international application(s) designating the United States of America, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT

material information as defined in Title 37, Code of Federal Regulations, § 1.56(a) which occurred between the filing date of the prior application and the national or PCT international filing date of this application.

U.S. PARENT APPLICATION OR PCT PARENT NUMBER	DATE OF FILING (day, month, year)	STATUS (patented, pending, abandoned)
09/281,017	30 MAR 99	Pending
09/449,159	24 NOV 99	Pending

I hereby claim the benefit under Title 35, United States Code § 119(e) of any United States provisional application(s) listed below:

U.S. PROVISIONAL APPLICATION NUMBER	DATE OF FILING (Day, Month, Year)
60/116,006	15 JAN 99

I hereby appoint the following attorneys to prosecute this application and to transact all business in the Patent and Trademark Office connected herewith:

George H. Gates	Registration No. 33,500
Victor G. Cooper	Registration No. 39,641
Anthony J. Orlor	Registration No. 41,232
Karen S. Canady	Registration No. 39,927
William J. Wood	Registration No. 42,236
Jason S. Feldmar	Registration No. 39,187

I hereby authorize them to act and rely on instructions from and communicate directly with the person/assignee/attorney/firm/ organization who/ which first sends/sent this case to them and by whom/which I hereby declare that I have consented after full disclosure to be represented unless/until I instruct Gates & Cooper to the contrary.

Please direct all correspondence in this case to the firm of Gates & Cooper at the address indicated below:

GATES & COOPER
Howard Hughes Center
6701 Center Drive West, Suite 1050
Los Angeles, CA 90045

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

(1)	Full Name Of Inventor	Family Name Abbott	First Given Name Shawn	Second Given Name D.
	Residence & Citizenship	City Calgary	State or Foreign Country Alberta	Country of Citizenship Canada
	Post Office Address	Post Office Address 305 Pinnacle Ridge Place, RR12	City Calgary	State & Zip Code/Country T3E 6W3/Canada
Signature of Inventor(1):				Date:
(2)	Full Name Of Inventor	Family Name Anderson	First Given Name Allan	Second Given Name D.
	Residence & Citizenship	City Cerritos	State or Foreign Country California	Country of Citizenship USA
	Post Office Address	Post Office Address 11158 Bertha Place	City Cerritos	State & Zip Code/Country California 90703/USA
Signature of Inventor(2):				Date:
(3)	Full Name Of Inventor	Family Name Goddling	First Given Name Patrick	Second Given Name N.
	Residence & Citizenship	City Lake Forest	State or Foreign Country California	Country of Citizenship USA
	Post Office Address	Post Office Address 22665 Shady Grove Circle	City Lake Forest	State & Zip Code/Country California 92630/USA
Signature of Inventor(3):				Date:
(4)	Full Name Of Inventor	Family Name Punt	First Given Name Maarten	Second Given Name G.
	Residence & Citizenship	City Lake Forest	State or Foreign Country California	Country of Citizenship USA
	Post Office Address	Post Office Address 24942 Paseo Arboleda	City Lake Forest	State & Zip Code/Country California 92630/USA
Signature of Inventor(4):				Date:
(5)	Full Name Of Inventor	Family Name Sotoodeh	First Given Name Mehdi	Second Given Name
	Residence & Citizenship	City Mission Viejo	State or Foreign Country California	Country of Citizenship Great Britain
	Post Office Address	Post Office Address 17 Paloma Drive	City Mission Viejo	State & Zip Code/Country California 92692/USA
Signature of Inventor(5):				Date:

§ 1.56 Duty to disclose information material to patentability.

(a) A patent by its very nature is affected with a public interest. The public interest is best served, and the most effective patent examination occurs when, at the time an application is being examined, the Office is aware of and evaluates the teachings of all information material to patentability. Each individual associated with the filing and prosecution of a patent application has a duty of candor and good faith in dealing with the Office, which includes a duty to disclose to the Office all information known to that individual to be material to patentability as defined in this section. The duty to disclose information exists with respect to each pending claim until the claim is canceled or withdrawn from consideration, or the application becomes abandoned. Information material to the patentability of a claim that is canceled or withdrawn from consideration need not be submitted if the information is not material to the patentability of any claim remaining under consideration in the application. There is no duty to submit information which is not material to the patentability of any existing claim. The duty to disclose all information known to be material to patentability is deemed to be satisfied if all information known to be material to patentability of any claim issued in a patent was cited by the Office or submitted to the Office in the manner prescribed by §§ 1.97(b)-(d) and 1.98. However, no patent will be granted on an application in connection with which fraud on the Office was practiced or attempted or the duty of disclosure was violated through bad faith or intentional misconduct. The Office encourages applicants to carefully examine:

- (1) prior art cited in search reports of a foreign patent office in a counterpart application, and
- (2) the closest information over which individuals associated with the filing or prosecution of a patent application believe any pending claim patentably defines, to make sure that any material information contained therein is disclosed to the Office.

(b) Under this section, information is material to patentability when it is not cumulative to information already of record or being made of record in the application, and

- (1) it establishes, by itself or in combination with other information, a prima facie case of unpatentability of a claim; or
- (2) it refutes, or is inconsistent with, a position the applicant takes in:
 - (i) opposing an argument of unpatentability relied on by the Office, or
 - (ii) asserting an argument of patentability.

A prima facie case of unpatentability is established when the information compels a conclusion that a claim is unpatentable under the preponderance of evidence, burden-of-proof standard, giving each term in the claim its broadest reasonable construction consistent with the specification, and before any consideration is given to evidence which may be submitted in an attempt to establish a contrary conclusion of patentability.

(c) Individuals associated with the filing or prosecution of a patent application within the meaning of this section are:

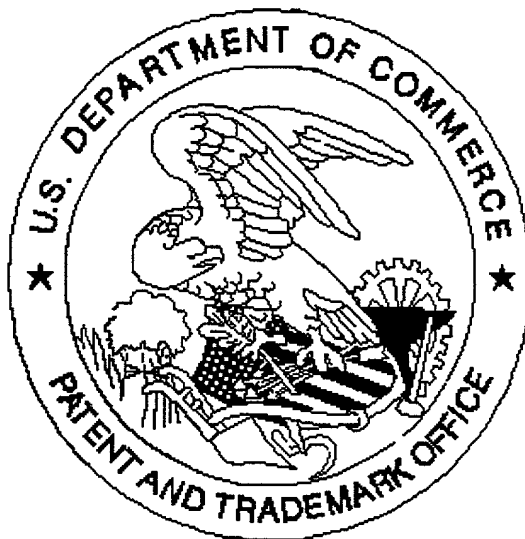
- (1) each inventor named in the application:
- (2) each attorney or agent who prepares or prosecutes the application; and

(3) every other person who is substantively involved in the preparation or prosecution of the application and who is associated with the inventor, with the assignee or with anyone to whom there is an obligation to assign the application.

(d) Individuals other than the attorney, agent or inventor may comply with this section by disclosing information to the attorney, agent, or inventor.

005490-061500

United States Patent & Trademark Office
Office of Initial Patent Examination -- Scanning Division



Application deficiencies were found during scanning:

☐ Page(s) _____ of _____ were not present
for scanning. (Document title)

☐ Page(s) _____ of _____ were not present
for scanning. (Document title)

there are 28 pages of specification enclosed

☐ Scanned copy is best available.